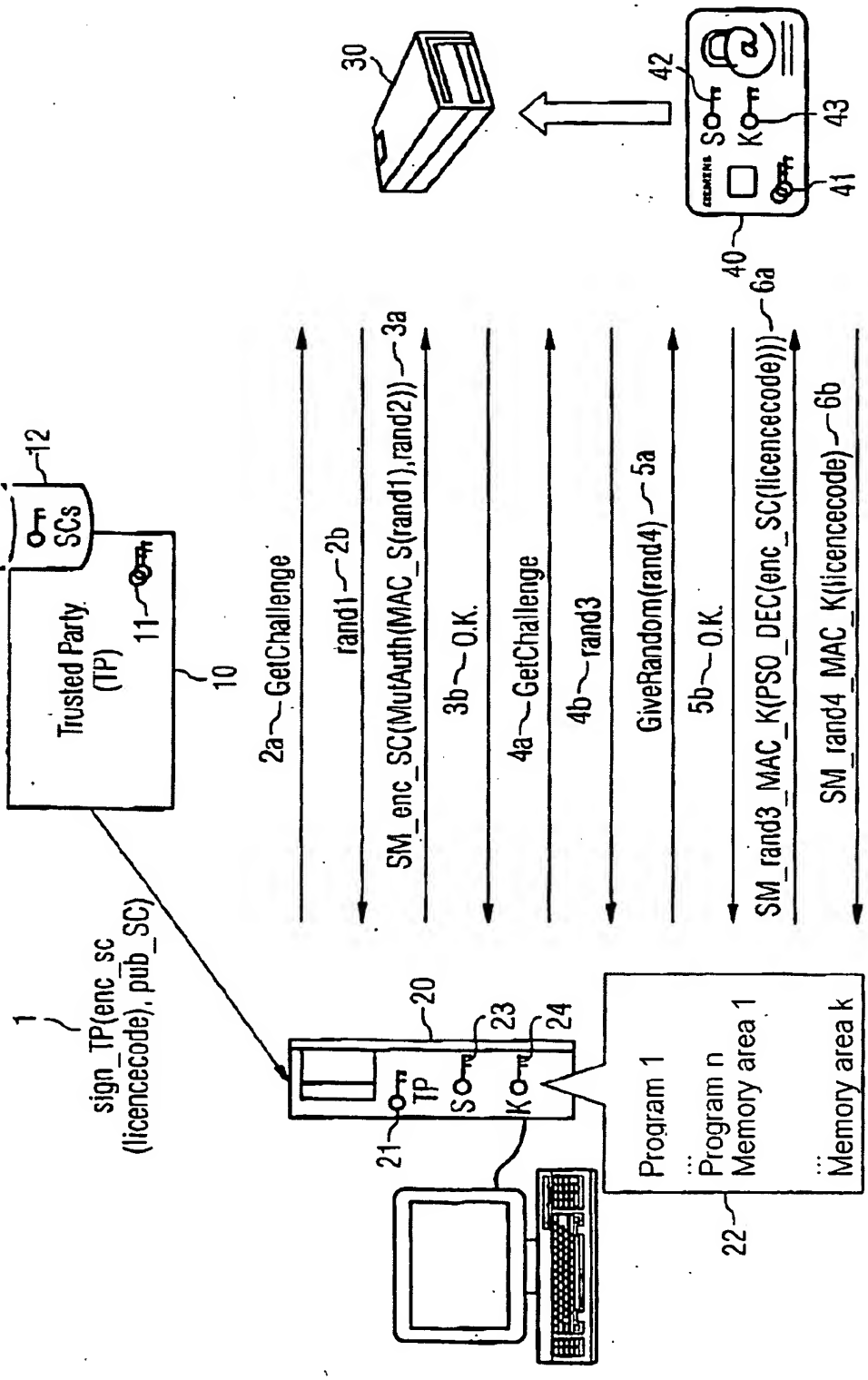
1
sign_TP(enc_sc (licencecode), pub_SC)
Trusted Party (TP)
10
11
12
SCs
2a GetChallenge
2b rand1
3a SM_enc_SC(MutAuth(MAC_S(rand1),rand2))
3b O.K.
4a GetChallenge
4b rand3
5a GiveRandom(rand4)
5b O.K.
6a SM_rand3_MAC_K(PSO_DEC(enc_SC(licencecode)))
6b SM_rand4_MAC_K(licencecode)
20
21
23
24
TP
S
K
22
Program 1
Program n
Memory area 1
Memory area k
30
40
41
42
43
S
K